Chapter 2 - Security Responsibilities

201 Security Planning

Planning for security is a management responsibility and shall be an integral part of any function or project undertaken in the Department. The most efficient and cost-effective method of instituting security measures for any facility or operation is through advance planning and continuous monitoring throughout the project, program, or activity. Once the essential security measures are determined, implementation of the measures is monitored to ensure the desired intent. Selecting, constructing, or modifying a facility without considering the security implications of employee safety and asset protection can result in costly modifications or retrofitting, considerable lost time, and liability for the Department. Receiving, processing, storing, or transmitting classified or sensitive information without adequate safeguards could result in damage to national security interests or a compromise of information entrusted to the Federal Government. Hiring individuals without the proper background investigation could also compromise critical or key departmental programs.

202 Roles and Responsibilities

Executive Order 12958, Classified National Security Information, as amended, confers the authority to originally classify information to designated agency heads and officials. In a subsequent Federal Register notice, the President conferred the authority to originally classify information at the Secret classification level to the Secretary of Commerce. E.O. 12958 further directs agency heads who originate or handle classified information to designate a senior agency official to direct and administer an agency-wide security program for all operating units within that agency. Departmental Organization Order (DOO) 20-6, Director for Security, designates the Director for Security as the "senior agency official" to direct and administer the Department of Commerce program implementing E.O. 12958, under which national security information is classified, safeguarded, and declassified. In addition, Executive Order 12968, Access to Classified Information, prescribes the policies, procedures, and standards that govern the granting of eligibility for access to national security information. The Director for Security establishes and oversees the process to evaluate background investigations, adjudicate issues, and grant eligibility for access to classified information for employees and other persons associated with the Department of Commerce. Besides protecting classified national security information and determining the eligibility for access to classified information, other laws, Executive Orders, and Federal regulations guide departmental security efforts to protect department personnel, facilities, and property and promote security education and awareness programs to achieve compliance with security policies and procedures. The guidance provided

below expands and supplements the responsibilities listed in DOO 20-6.

A. Director for Security.

1. The Director for Security (the "Director") serves as the focal point for all security matters in the Department and has Department-wide staff management responsibility for establishing policies and procedures for: personnel security; the safeguarding of classified and sensitive documents and information; the protection of Department personnel, facilities, and property; threat analysis and security risk assessments; emergency actions and preparedness; communications security; operations security; security education, awareness, and training; and compliance with security policies and procedures. The Director may approve or deny requests for exceptions to the procedural requirements of the Security Manual.

2. The Director is responsible for advising and assisting heads of operating units in performing their security responsibilities. Additionally, the Director provides security services when it is more practical or economical to consolidate them at Department level. (For the purpose of administering Departmental security programs, the Office of the Secretary is considered an "operating unit" and is subject to policy and procedural requirements levied on all other DOC units. The Director for Security shall serve as the Security Officer for the Office of the Secretary.)

3. The Director establishes the Department of Commerce Security Council composed of representatives from each operating unit to coordinate security measures in the Department. Operating unit representatives communicate security requirements to their respective units, exchange security-related information, and coordinate security services. Designating an employee to assist in performing security activities will not relieve the operating unit head, senior facility manager, or servicing security officer of their responsibilities.

4. The Director may delegate those authorities pertaining to security matters listed in DOO 20-6 to the Deputy Director for Security or other senior managers as appropriate.

B. Heads of Operating Units. The head of each operating unit, defined by DOO 1-1, "Mission and Organization of the Department of Commerce," as amended, is responsible for ensuring the security of the personnel, property, facilities, and information in their respective organizations in accordance with applicable laws, regulations, Executive Orders, and directives.

1. The head of each operating unit is responsible for developing and implementing measures to protect personnel, property, facilities, and information in their respective organization in accordance with applicable laws, regulations, Executive Orders, and directives. The head of each operating unit is responsible for implementing security policies and procedures

described in the Security Manual. Servicing security officers will provide administrative support to the operating units.

2. The head of each operating unit, in consultation with the servicing human resources manager, shall ensure that the unit's personnel suitability matters comply with appropriate laws and regulations. In particular, the head of an operating unit must ensure that each position within the operating unit is designated with the appropriate position sensitivity or risk level in accordance with the position sensitivity and risk criteria set forth in 5 CFR § 731 and § 732, DAO 202-731, Handbook on Suitability, and the Security Manual.

3. The head of each operating unit shall ensure that employees in their organization receive periodic training regarding safeguarding national security and sensitive information in accordance with Chapter 3, Security Education and Awareness, and Chapter 41, Sensitive and Administratively Controlled Information, of the Security Manual.

4. The head of each operating unit will appoint a representative to the Department's Security Council. The representative will communicate security requirements from their respective operating units, exchange security-related information, and coordinate security services in their organization.

C. Human Resources Managers. Human resources managers or their designee are responsible for administering the personnel suitability investigations process required within their jurisdiction in accordance with appropriate laws and regulations. Operating unit managers, in consultation and concurrence with human resources managers, are the adjudicating authorities for their respective organizations. Human resources offices shall advise the Office of Security, through the servicing security officer, when they become aware of information in a suitability investigation that could cause harm to the national security interests of the United States.

D. Servicing Security Officers.

1. Department of Commerce security officers implement departmental security program activities in operating units on behalf of the Director for Security. Security officers provide security guidance, service, and support to the bureaus, operating units, and departmental offices under their jurisdiction; implement security policies and procedures issued by the Office of Security; and coordinate any safeguarding requirements that specifically pertain to an operating unit with the appropriate head of an operating unit.

2. Servicing security officers may formulate and issue supplementary instructions for their servicing area concerning personnel, information, and physical security matters. Each security officer must actively administer education and inspection programs for each office

within their service area that processes, handles, or stores national security information.

E. Facility and Senior Office Managers. Department of Commerce facility and senior office managers are responsible for ensuring the security of the personnel, property, facilities, and information in their respective facilities in accordance with applicable laws, regulations, Executive Orders, and directives. Security officers providing client services to operating units will assist facility managers in carrying out these responsibilities.

F. Security Contacts. The head of an operating unit, departmental office, or other departmental organization that does not have a Security Specialist, GS-0080, assigned as a servicing security officer will appoint a liaison to the Office of Security to act as a security point-of-contact for all security matters in their organization. The security contact may perform collateral duties that involve responsibilities such as initiating and processing requests for background investigations for applicants and employees in their organization; forwarding up-to-date national security information to supervisors and employees in their organization; assisting senior facility managers in coordinating physical security risk assessments of their facility; assisting the head of the organization in ensuring that all persons with security clearances receive an annual refresher security briefing; or requesting assistance from the Office of Security regarding security matters.

G. Supervisors. Supervisors are responsible for ensuring all applicable security policies and procedures are implemented in their organization.

1. Supervisors will assign risk and sensitivity designations to all positions under their authority in accordance with position designation criteria to ensure individuals filling those positions receive the appropriate background investigation.

2. When an employee requires access to national security information, the supervisor will forward a completed CD-79, Request for Security Clearance, through the servicing security officer to the Office of Security, indicating the level of clearance needed, and a statement justifying need for the access.

3. If a supervisor becomes aware of any derogative information concerning an employee that indicates continued access is no longer in the interest of the national security, he or she must notify the Office of Security so that an inquiry or investigation may be initiated to determine the validity of the information and the need to suspend, revoke, deny, or restrict the employee's access to national security information. Chapter 13, Security Adjudication Criteria, provides examples of information used to determine an individual's eligibility for access to national security information.

H. Employees and Other Individuals.

1. Employees and other individuals associated with the Department must become familiar with pertinent security regulations. Furthermore, individuals with security clearances must comply with standards of conduct when holding positions of trust as stated in E.O. 11222, Standards of Conduct, and the U.S. Department of Commerce, Standards of Conduct for Commerce Employees handbook. Individuals must recognize and avoid the kind of personal behavior that could result in their ineligibility for continued assignment to a position of trust.

2. All employees and other individuals who have been given access to classified or sensitive information must abide by the applicable guidance and directives concerning its maintenance and protection as prescribed in Section III, National Security Information, and Chapter 41, Sensitive and Administratively Controlled Information.

3. Each employee and other individuals will advise their supervisor, servicing security officer, or operating unit's security contact when they become aware of information about any departmental employee or individual associated with the Department who could potentially cause damage to the national security interests of the United States.

203 Administrative and Judicial Action

Failure to comply with the policies or procedures set forth in the Security Manual may result in written notice of violation and other administrative action, as appropriate, under the provisions of applicable statutes, Executive Orders, and regulations. The Office of Security shall recommend disciplinary action based on DAO 202-751, Discipline, against any employee or contractor in the Department determined to have been responsible for violation of applicable policies or procedures. Actions by an employee or contractor that indicate a disregard for the national security as determined by the Office of Security may result in suspension and subsequent revocation of the individual's security clearance. If an employee violates a criminal statute pertaining to national security, the matter will be referred to the Office of the Inspector General for possible referral to the Department of Justice.

204 After Hours Security Checks and Self Inspections

Servicing security officers and security contacts, in consultation with local office managers, will conduct periodic, after-hours checks and self-inspections of areas that handle, process, and store national security information to ensure that the inspected organization is in compliance with departmental security policies and procedures. The Office of Security shall conduct a continuous after-hours security inspection program to ensure compliance in each operating units. This will include office areas within Office of Security.